

### CLAIMS

1. A router device which can set a first cryptographic tunnel to a repeating node device, comprising:
  - a. a first unit to receive encrypted packets for a terminal;
  - b. a second unit to transmit said encrypted packets through a first cryptographic tunnel for said terminal to a repeating node; and
  - c. a third unit to form a second cryptographic tunnel between said router device and an end node device when traffic of said encrypted packets has exceeded a first threshold value.
2. A router device, as per claim 1, further comprising an input I/F unit, a routing unit, a IPSec processing unit, and an output I/F unit.
3. A router device, as per claim 2, wherein said IPSec processing unit further comprises an Security Policy Database (SPD), an Security Association Database (SAD), a Default/Direct (DDT), and a traffic-monitoring unit.
4. A router device, as per claim 3, wherein said cryptographic tunnel is formed by consulting an SPD, an SAD, and a DDT.

5. A router device, as per claim 3, wherein said SPD stores security policy information comprising: a link number, an encryption policy, a protocol, and a direct flag and is searched using a start point IP address and an end point IP address extracted from a packet.
6. A router device, as per claim 4, wherein said first and second cryptographic tunnels are selected by selecting a link number.
7. A router device, as per claim 4, wherein said SPD comprises encryption policy further comprising an encryption, non-encryption, and destruction policy.
8. A router device, as per claim 3, wherein said SAD stores information comprising: an end point IP address, a link number, class of IPsec protocol, an SPI value, Security Association parameters (SA) parameters, and a direct indication and is searched using an end point IP address.
9. A router device, as per claim 3, wherein said traffic-monitoring unit

- a. determines whether packets are transferred over a default or direct route cryptographic tunnel,
- b. if packets are transferred over a default route cryptographic tunnel
  - i. said traffic-monitoring process counts the number of packets received over said cryptographic tunnel during a preset amount of time,
  - ii. if the number of packets counted during said preset amount of time is below a threshold value, a direct route cryptographic tunnel connection request is set and a default route packet counter is cleared, or
  - iii. if the number of packets counted during said preset amount of time is equal to or above said threshold value, said default route packet counter is cleared, and
- c. If packets are transferred over a direct route cryptographic tunnel
  - i. said traffic-monitoring process counts the number of packets received over said cryptographic tunnel during a preset amount of time,
  - ii. if the number of packets counted during said preset amount of time is below a threshold value, direct route packet counter is cleared, or
  - iii. if the number of packets counted during said preset amount of time is equal to or above said threshold value, said direct route packet counter is cleared, and a default route cryptographic tunnel connection request is set.

10. A router device, as per claim 9, wherein said direct route cryptographic tunnel connection request further comprises steps of:
- a. updating an SPD by changing an identification parameter to have a direct route value,
  - b. deleting information from an SAD where a link number corresponding to a said cryptographic connection is used to identify a row in said SAD to delete, and
  - c. sending a message to provide notification of cryptographic tunnel connection termination.
11. A router device, as per claim 8, wherein said security association database (SAD) indicates a direct or a default route corresponding to a first and second cryptographic tunnel, respectively.
12. A router device, as per claim 3, wherein said DDT stores information comprising: a destination IP address, a transfer destination IP address, an encryption policy, an identification flag, and a drive request and is searched using a destination IP address.
13. A router device, as per claim 1, wherein said first cryptographic tunnel is switched to said second cryptographic tunnel when traffic through said first cryptographic tunnel exceeds a first threshold value.

14. A router device, as per claim 13, wherein said switched second cryptographic tunnel is switched back to said first cryptographic tunnel when traffic through said second cryptographic tunnel is lower than a second threshold value.

15. A router device, as per claim 1, further comprising a fourth unit to include information indicative of a request to switch between said first cryptographic tunnel and said second cryptographic tunnel to perform a switching process between said first cryptographic tunnel and said second cryptographic tunnel.

16. A cryptographic communication system having a repeating node device, a start node device which can set a first cryptographic tunnel to said repeating node device, and an end node device, comprising:

- a. a first node device comprising:
  - i. a first unit to receive packets for a terminal;
  - ii. a second unit to transmit the encrypted received packets through the first cryptographic tunnel; and
  - iii. a third unit to form a second cryptographic tunnel between the first node device and the end node device when traffic of the encrypted received packets has exceeded a first threshold value;

- b. said repeating node device to decrypt a received encrypted packets from said first node and transmit received encrypted packets to said terminal; and
- c. the end node device to decode the received encrypted packets and transmit the received encrypted packets to the terminal.

17. A method for cryptographic communication comprising:

- a. receiving packets for a terminal at a first node;
- b. transmitting the encrypted received packets to a repeating node over a first cryptographic tunnel;
- c. decoding the encrypted received packet at the repeating node;
- d. transmitting the encrypted decoded-packet to an end node; and
- e. forming a second cryptographic tunnel between a start node and an end node when received packet traffic transferred over a first cryptographic tunnel has exceeded the first threshold value.